

**UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION**

**CHRISTOPHER EDWARDS,
individually, and on behalf of all
others similarly situated,**

Plaintiff

v.

**TRC STAFFING SERVICES INC.
d/b/a TRC TALENT SOLUTIONS,**

Defendant.

Case No. _____

CLASS ACTION COMPLAINT AND JURY DEMAND

Christopher Edwards (“Plaintiff”), through his attorneys, individually and on behalf of all others similarly situated, brings this Class Action Complaint against Defendant TRC Staffing Services Inc. d/b/a TRC Talent Solutions (“TRC” or “Defendant”), and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities. Plaintiff alleges the following on information and belief—except as to his own actions, counsel’s investigations, and facts of public record.

NATURE OF ACTION

1. This class action arises from Defendant’s failure to protect highly sensitive data.

2. Defendant is a staffing provider headquartered in Atlanta, Georgia.

3. As such, Defendant stores a litany of highly sensitive personal identifiable information (“PII”) about its employees. But Defendant lost control over that data when cybercriminals infiltrated its insufficiently protected computer systems in a data breach (the “Data Breach”)

4. It is unknown precisely how long the cybercriminals had access to Defendant’s network before the breach was discovered. In other words, Defendant had no effective means to prevent, detect, stop, or mitigate breaches of its systems—thereby allowing cybercriminals unrestricted access to employees’ PII.

5. On information and belief, cybercriminals were able to breach Defendant’s systems because Defendant failed to adequately train its employees on cybersecurity and failed to maintain reasonable security safeguards or protocols to protect the Class’s PII. In short, Defendant’s failures placed the Class’s PII in a vulnerable position—rendering them easy targets for cybercriminals.

6. Plaintiff is a Data Breach victim, having received a breach. *See* Ex. A. He brings this class action on behalf of himself, and all others harmed by Defendant’s misconduct.

7. The exposure of one’s PII to cybercriminals is a bell that cannot be unrung. Before this data breach, Plaintiff’s and the Class’s private information was

exactly that—private. Not anymore. Now, their private information is forever exposed and unsecure.

PARTIES

8. Plaintiff, Christopher Edwards, is natural person and citizen of Georgia. He resides in Lawrenceville, Georgia where he intends to remain.

9. Defendant, TRC Staffing Services Inc. (d/b/a TRC Talent Solutions) is a Domestic Profit Corporation with its principal place of business at 5909 Peachtree Dunwoody Road, Suite D-1100, Atlanta, Georgia 30328, USA.

JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of \$5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

11. This Court has general personal jurisdiction over Defendant TRC because Defendant's principal place of business is in this District and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

12. Venue is proper under 18 U.S.C. § 1391(b)(1) because Defendant's principal place of business is in this District.

BACKGROUND

Defendant Collected and Stored the PII of Plaintiff and the Class

13. Defendant is a staffing services provider with fifteen offices nationwide.¹ In particular, Defendant has offices in: Florida, Georgia, Missouri, North Carolina, Ohio, Pennsylvania, and South Carolina.²

14. Defendant advertises the following:

- a. “Business has undergone a dramatic transformation. In every industry, your success depends on how you embrace and maximize recent workforce changes – as well as the changes yet to come. That’s where TRC makes a difference.”³
- b. “TRC careers deliver significant benefits, advantages and opportunities.”⁴
- c. “Continual improvement is fundamental to our organizational success, and we’re just as dedicated to helping each of our employees continually grow as professionals.”⁵

¹ *Locations*, TRC SOLUTIONS, <https://trctalent.com/location/> (last accessed Jun. 3, 2024).

² *Id.*

³ *Home*, TRC SOLUTIONS, <https://trctalent.com/> (last accessed Jun. 3, 2024).

⁴ *Work For TRC*, TRC SOLUTIONS, <https://trctalent.com/about/> (last accessed Jun. 3, 2024)

⁵ *Work for TRC*, TRC SOLUTIONS, <https://trctalent.com/work-for-trc/> (last accessed Jun. 3, 2024).

d. Prospective employees should expect to succeed, “as each individual succeeds, we all succeed.”⁶

15. In collecting and maintaining the PII of its employees, Defendant impliedly agreed it would safeguard the data in accordance with its internal policies, state law, and federal law. After all, Plaintiff and Class members themselves took reasonable steps to secure their PII.

16. As part of its business, Defendant receives and maintains the PII of thousands of employees. In doing so, Defendant implicitly promises to safeguard their PII.

17. Under state and federal law, businesses like Defendant have duties to protect its current and former employees’ PII and to notify them about breaches.

18. Defendant recognizes these duties. For one, Defendant declares—in its Privacy Policy—that “We maintain robust technological and organizational security measures to safeguard your personal information.”⁷ Similarly, Defendant states that “Our policy ensures that only individuals with a legitimate business need have access to your personal information.”⁸

⁶ *Id.*

⁷ *Privacy Policy*, TRC SOLUTIONS, <https://trctalent.com/privacy-policy/> (last accessed Jun. 3, 2024).

⁸ *Id.*

Defendant's Data Breach

19. On March 25, 2024, Defendant was hacked by cybercriminals.⁹ But Defendant did not discover the breach until May 9, 2024—45 days later.¹⁰

20. Because of Defendant's Data Breach, at least the following types of PII were compromised:

- a. Names,
- b. Social Security numbers.¹¹

21. In total, Defendant injured at least 158,593 persons—via the exposure of their PII—in the Data Breach.¹² Upon information and belief, these 158,593 persons include current and former employees of Defendant.

22. And yet, Defendant waited over *60 days* before it began notifying the class (notifications began to be sent out on May 24, 2024).¹³

23. Thus, Defendant kept the Class in the dark—thereby depriving the Class of the opportunity to try and mitigate their injuries in a timely manner.

24. And when Defendant did notify Plaintiff and the Class of the Data Breach, Defendant acknowledged that the Data Breach created a present, continuing,

⁹ *Data Breach Notifications*, MAINE ATTY GEN., <https://apps.web.maine.gov/online/aeviewer/ME/40/1adfdecc-df2a-47a6-93bc-ef5a7ad1ac7a.shtml> (last visited Jun. 3, 2024).

¹⁰ *Id.*

¹¹ *Id.*

¹² *Id.*

¹³ *Id.*

and significant risk of suffering identity theft, warning Plaintiff and the Class to spend time and money to prevent further harm:

- a. “remain vigilant against incidents of identity theft and fraud;”
- b. “review[] your account and free credit reports for suspicious activity and to detect errors;”
- c. “enroll in the complementary credit-monitoring services available to you;”
- d. Gave “additional information and resources included in the enclosed *Steps You Can Take to Help Protect Personal Information*.”¹⁴

25. Defendant failed in its duties when its inadequate security practices caused the Data Breach. In other words, Defendant’s negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII. And thus, Defendant caused widespread injury and monetary damages.

26. Since the breach, Defendant has “[taken] steps to secure our systems and initiated a comprehensive response.” And “reviewed our security policies and procedures and [have] implement[ed] additional security measures to reduce the risk of similar future events.”¹⁵ But this is too little too late. Simply put, these measures—

¹⁴ *Id.*; Ex. A.

¹⁵ *Id.*

which Defendant now recognizes as necessary—should have been implemented *before* the Data Breach.

27. On information and belief, Defendant failed to adequately train its employees on reasonable cybersecurity protocols or implement reasonable security measures.

28. Further, the Notice of Data Breach shows that Defendant cannot—or will not—determine the full scope of the Data Breach, as Defendant has been unable to determine precisely what information was stolen and when. *See* Ex. A.

29. Defendant has done little to remedy its Data Breach. True, Defendant has offered some victims credit monitoring and identity related services. But upon information and belief, such services are wholly insufficient to compensate Plaintiff and Class members for the injuries that Defendant inflicted upon them.

30. Because of Defendant’s Data Breach, the sensitive PII of Plaintiff and Class members was placed into the hands of cybercriminals—inflicting numerous injuries and significant damages upon Plaintiff and Class members.

A Notorious Cybercriminal Group Now Has the PII of Plaintiff and the Class

31. Since the Data Breach occurred, a notorious cybercriminal group called “BlackSuit” has claimed responsibility.¹⁶ Thus far, BlackSuit has:

¹⁶ *The Vulnerabilities and Tactics Behind the Ransomware Attack on TRC Talent Solutions*, HALYCON, <https://ransomwareattacks.halcyon.ai/attacks/the->

- a. claimed to have accessed and stolen data from Defendant—including highly sensitive PII;
- b. and has threatened to *publish the data* if a ransom is not paid.¹⁷

32. BlackSuit is a particularly sophisticated and dangerous criminal group, with indications that they are a rebranding effort of a ransomware gang called “Royal”. It has been profiled by the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA).¹⁸ In a joint advisory, these federal agencies issued the following warnings:

- a. “Phishing emails are among the most successful vectors for initial access by Royal threat actors. There are indications that Royal may be preparing for a re-branding effort and/or a spinoff variant. BlackSuit ransomware shares a number of identified coding characteristics similar to Royal;”
- b. “Since approximately September 2022, cyber threat actors have compromised U.S. and international organizations with Royal ransomware;”

vulnerabilities-and-tactics-behind-the-ransomware-attack-on-trc-talent-solutions (last accessed Jun. 3, 2024).

¹⁷ *Id.*

¹⁸ *CISA, FBI warn that Royal Ransomware gang may rebrand as ‘BlackSuit’*, THE RECORD, <https://therecord.media/cisa-fbi-warn-royal-ransomware-gang-rebrands-blacksuit> (last accessed Jun. 3, 2024)

- c. “After gaining access to victims’ networks, Royal actors disable antivirus software and exfiltrate large amounts of data before ultimately deploying the ransomware and encrypting the systems;”
- d. “Royal actors have made ransom demands ranging from approximately \$1 million to \$11 million USD in Bitcoin;”
- e. “In observed incidents, Royal actors do not include ransom amounts and payment instructions as part of the initial ransom note. Instead, the note, which appears after encryption, requires victims to directly interact with the threat actor via a .onion URL (reachable through the Tor Browser).”¹⁹

Plaintiff’s Experiences and Injuries

- 33. Plaintiff Christopher Edwards is a former employee of Defendant.
- 34. As a condition of employment, Defendant required Plaintiff to provide it with his PII. Defendant thus obtained and maintained Plaintiff’s PII.
- 35. As a result, Plaintiff Christopher Edwards was injured by Defendant’s Data Breach.

¹⁹ #StopRansomware: Royal Ransomware, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY, <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-061a> (last accessed Jun. 3, 2024)

36. Plaintiff does not recall ever learning that his information was compromised in a data breach incident—other than the breach at issue here.

37. Plaintiff received a Notice of Data Breach dated May 30th, 2024.

38. Through its Data Breach, Defendant compromised Plaintiff's name and Social Security number.

39. On information and belief, Plaintiff's PII was obtained by BlackSuit and has been, or will be, published on the dark web.

40. Plaintiff has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft. After all, Defendant directed Plaintiff to take those steps in its breach notice. *See* Ex. A.

41. Plaintiff fears for his personal financial security and worries about what information was exposed in the Data Breach.

42. Because of Defendant's Data Breach, Plaintiff has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff's injuries are precisely the type of injuries that the law contemplates and addresses.

43. Plaintiff suffered actual injury from the exposure and theft of his PII—which violates his rights to privacy.

44. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

45. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant’s Data Breach placed Plaintiff’s PII right in the hands of criminals.

46. Because of the Data Breach, Plaintiff anticipates spending considerable amounts of time and money to try and mitigate his injuries.

47. Today, Plaintiff has a continuing interest in ensuring that his PII—which, upon information and belief, remains backed up in Defendant’s possession—is protected and safeguarded from additional breaches.

Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

48. Because of Defendant’s failure to prevent the Data Breach, Plaintiff and Class members suffered—and will continue to suffer—damages. These damages include, *inter alia*, monetary losses, lost time, anxiety, and emotional distress. Also, they suffered or are at an increased risk of suffering:

- a. loss of the opportunity to control how their PII is used;
- b. diminution in value of their PII;
- c. compromise and continuing publication of their PII;

- d. out-of-pocket costs from trying to prevent, detect, and recovery from identity theft and fraud;
- e. lost opportunity costs and wages from spending time trying to mitigate the fallout of the Data Breach by, *inter alia*, preventing, detecting, contesting, and recovering from identify theft and fraud;
- f. delay in receipt of tax refund monies;
- g. unauthorized use of their stolen PII; and
- h. continued risk to their PII—which remains in Defendant’s possession—and is thus as risk for futures breaches so long as Defendant fails to take appropriate measures to protect the PII.

49. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to \$1,000.00 depending on the type of information obtained.

50. The value of Plaintiff and Class’s PII on the black market is considerable. Stolen PII trades on the black market for years. And criminals frequently post and sell stolen information openly and directly on the “dark web”—further exposing the information.

51. It can take victims years to discover such identity theft and fraud. This gives criminals plenty of time to sell the PII far and wide.

52. One way that criminals profit from stolen PII is by creating comprehensive dossiers on individuals called “Fullz” packages. These dossiers are both shockingly accurate and comprehensive. Criminals create them by cross-referencing and combining two sources of data—first the stolen PII, and second, unregulated data found elsewhere on the internet (like phone numbers, emails, addresses, etc.).

53. The development of “Fullz” packages means that the PII exposed in the Data Breach can easily be linked to data of Plaintiff and the Class that is available on the internet.

54. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and Class members, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff and other Class members’ stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

55. Defendant disclosed the PII of Plaintiff and Class members for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiff and Class members to people engaged

in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII.

56. Defendant's failure to promptly and properly notify Plaintiff and Class members of the Data Breach exacerbated Plaintiff and Class members' injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

Defendant Knew—Or Should Have Known—of the Risk of a Data Breach

57. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in recent years.

58. In 2021, a record 1,862 data breaches occurred, exposing approximately 293,927,708 sensitive records—a 68% increase from 2020.²⁰ Of the 1,862 recorded data breaches, 330 of them, or 17.7% were in the medical or healthcare industry.²¹ Those 330 reported breaches exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.²²

59. Indeed, cyberattacks have become so notorious that the Federal Bureau

²⁰ See *2021 Data Breach Annual Report*, IDENTITY THEFT RESOURCE CENTER (Jan. 2022) <https://notified.idtheftcenter.org/s/>.

²¹ *Id.*

²² *Id.*

of Investigation (“FBI”) and U.S. Secret Service issue warnings to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, “[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly.”²³

60. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.²⁴

61. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant’s industry, including Defendant.

Defendant Failed to Follow FTC Guidelines

62. According to the Federal Trade Commission (“FTC”), the need for data security should be factored into all business decision-making. Thus, the FTC issued numerous guidelines identifying best data security practices that businesses—like Defendant—should use to protect against unlawful data exposure.

²³ Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), <https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware>.

²⁴ See Maria Henriquez, *Iowa City Hospital Suffers Phishing Attack*, SECURITY MAGAZINE (Nov. 23, 2020), <https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack> (last visited July 31, 2022).

63. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*. There, the FTC set guidelines for what data security principles and practices businesses must use.²⁵ The FTC declared that, *inter alia*, businesses must:

- a. protect the personal customer information that they keep;
- b. properly dispose of personal information that is no longer needed;
- c. encrypt information stored on computer networks;
- d. understand their network's vulnerabilities; and
- e. implement policies to correct security problems.

64. The guidelines also recommend that businesses watch for the transmission of large amounts of data out of the system—and then have a response plan ready for such a breach.

65. Furthermore, the FTC explains that companies must:

- a. not maintain information longer than is needed to authorize a transaction;
- b. limit access to sensitive data;
- c. require complex passwords to be used on networks;

²⁵ *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (Oct. 2016) https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

- d. use industry-tested methods for security;
- e. monitor for suspicious activity on the network; and
- f. verify that third-party service providers use reasonable security measures.

66. The FTC brings enforcement actions against businesses for failing to protect customer data adequately and reasonably. Thus, the FTC treats the failure—to use reasonable and appropriate measures to protect against unauthorized access to confidential consumer data—as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

67. In short, Defendant’s failure to use reasonable and appropriate measures to protect against unauthorized access to employees’ data constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Failed to Follow Industry Standards

68. Several best practices have been identified that—at a *minimum*—should be implemented by businesses like Defendant. These industry standards include: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption (making data

unreadable without a key); multi-factor authentication; backup data; and limiting which employees can access sensitive data.

69. Other industry standard best practices include: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

70. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

71. These frameworks are applicable and accepted industry standards. And by failing to comply with these accepted standards, Defendant opened the door to the criminals—thereby causing the Data Breach.

CLASS ACTION ALLEGATIONS

72. Plaintiff brings this nationwide class action on behalf of himself and on

behalf of others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

73. The nationwide Class that Plaintiff seeks to represent is defined as follows:

All United States residents whose PII was compromised in the Data Breach discovered by TRC in May 2024, including all those who received notice of the breach.

74. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

75. Plaintiff reserves the right to amend the class definition.

76. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of his claims on class-wide bases using the same evidence as would be used to prove those elements in individual actions asserting the same claims.

77. Ascertainability. All members of the proposed Class are readily ascertainable from information in Defendant's custody and control. After all, Defendant already identified some individuals and sent them data breach notices.

78. Numerosity. The Class members are so numerous that joinder of all Class members is impracticable. Upon information and belief, the proposed Class includes at least 158,593 members.

79. Typicality. Plaintiff's claims are typical of Class members' claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

80. Adequacy. Plaintiff will fairly and adequately protect the proposed Class's common interests. his interests do not conflict with Class members' interests. And Plaintiff has retained counsel—including lead counsel—that is experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf.

81. Commonality and Predominance. Plaintiff's and the Class's claims raise predominantly common fact and legal questions—which predominate over any questions affecting individual Class members—for which a class wide proceeding can answer for all Class members. In fact, a class wide proceeding is necessary to answer the following questions:

- a. if Defendant had a duty to use reasonable care in safeguarding Plaintiff's and the Class's PII;

- b. if Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- c. if Defendant were negligent in maintaining, protecting, and securing PII;
- d. if Defendant breached contract promises to safeguard Plaintiff and the Class's PII;
- e. if Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;
- f. if Defendant's Breach Notice was reasonable;
- g. if the Data Breach caused Plaintiff and the Class injuries;
- h. what the proper damages measure is; and
- i. if Plaintiff and the Class are entitled to damages, treble damages, and or injunctive relief.

82. Superiority. A class action is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class members are relatively small compared to the burden and expense that individual litigation against Defendant would require. Thus, it would be practically impossible for Class members, on an individual basis, to obtain effective redress for their injuries. Not only would

individualized litigation increase the delay and expense to all parties and the courts, but individualized litigation would also create the danger of inconsistent or contradictory judgments arising from the same set of facts. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, ensures economies of scale, provides comprehensive supervision by a single court, and presents no unusual management difficulties.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiff and the Class)

83. Plaintiff incorporates by reference Paragraphs 1 through 82 as if fully set forth herein.

84. Plaintiff and the Class entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their PII, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

85. Defendant owed a duty of care to Plaintiff and Class members because it was foreseeable that Defendant's failure—to use adequate data security in accordance with industry standards for data security—would compromise their PII in a data breach. And here, that foreseeable danger came to pass.

86. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if their PII was wrongfully disclosed.

87. Defendant owed these duties to Plaintiff and Class members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security practices. After all, Defendant actively sought and obtained Plaintiff and Class members' PII.

88. Defendant owed—to Plaintiff and Class members—at least the following duties to:

- a. exercise reasonable care in handling and using the PII in its care and custody;
- b. implement industry-standard security procedures sufficient to reasonably protect the information from a data breach, theft, and unauthorized;
- c. promptly detect attempts at unauthorized access;
- d. notify Plaintiff and Class members within a reasonable timeframe of any breach to the security of their PII.

89. Thus, Defendant owed a duty to timely and accurately disclose to Plaintiff and Class members the scope, nature, and occurrence of the Data Breach. After all, this duty is required and necessary for Plaintiff and Class members to take appropriate measures to protect their PII, to be vigilant in the face of an increased

risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

90. Defendant also had a duty to exercise appropriate clearinghouse practices to remove PII it was no longer required to retain under applicable regulations.

91. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII of Plaintiff and the Class involved an unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the criminal acts of a third party.

92. Defendant's duty to use reasonable security measures arose because of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential PII, a necessary part of obtaining services from Defendant.

93. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendant held vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII—whether by malware or otherwise.

94. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiff and Class members' and the importance of exercising reasonable care in handling it.

95. Defendant improperly and inadequately safeguarded the PII of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

96. Defendant breached these duties as evidenced by the Data Breach.

97. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and Class members' PII by:

- a. disclosing and providing access to this information to third parties and
- b. failing to properly supervise both the way the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

98. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII of Plaintiff and Class members which actually and proximately caused the Data Breach and Plaintiff and Class members' injury.

99. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and Class members, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff and Class members' injuries-in-fact.

100. Defendant has admitted that the PII of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

101. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and Class members have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

102. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and Class members actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

SECOND CAUSE OF ACTION
Negligence *per se*
(On Behalf of Plaintiff and the Class)

103. Plaintiff incorporates by reference Paragraphs 1 through 82 as if fully set forth herein.

104. Under the FTC Act, 15 U.S.C. § 45, Defendant had a duty to use fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class members' PII.

105. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted, and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect the PII entrusted to it. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff and the Class members' sensitive PII.

106. Defendant breached its respective duties to Plaintiff and Class members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII.

107. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

108. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Class.

109. But for Defendant's wrongful and negligent breach of its duties owed, Plaintiff and Class members would not have been injured.

110. The injury and harm suffered by Plaintiff and Class members was the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their PII.

111. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

THIRD CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

112. Plaintiff incorporates by reference Paragraphs 1 through 82 as if fully set forth herein.

113. Plaintiff and Class members were required to provide their PII to Defendant as a condition of receiving medical services provided by Defendant. Plaintiff and Class members provided their PII to Defendant or its third-party agents in exchange for Defendant's medical services.

114. Plaintiff and Class members reasonably understood that a portion of the funds they paid Defendant would be used to pay for adequate cybersecurity measures.

115. Plaintiff and Class members reasonably understood that Defendant would use adequate cybersecurity measures to protect the PII that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

116. Plaintiff and the Class members accepted Defendant's offers by disclosing their PII to Defendant or its third-party agents in exchange for medical services.

117. In turn, and through internal policies, Defendant agreed to protect and not disclose the PII to unauthorized persons.

118. In its Privacy Policy, Defendant represented that they had a legal duty to protect Plaintiff's and Class Member's PII.

119. Implicit in the parties' agreement was that Defendant would provide Plaintiff and Class members with prompt and adequate notice of all unauthorized access and/or theft of their PII.

120. After all, Plaintiff and Class members would not have entrusted their PII to Defendant or its third-party agents in the absence of such an agreement with Defendant.

121. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant.

122. The covenant of good faith and fair dealing is an element of every contract. Thus, parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—and not merely the letter—of the bargain. In short, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

123. Subterfuge and evasion violate the duty of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or consist of inaction. And fair dealing may require more than honesty.

124. Defendant materially breached the contracts it entered with Plaintiff and Class members by:

- a. failing to safeguard their information;
- b. failing to notify them promptly of the intrusion into its computer systems that compromised such information.
- c. failing to comply with industry standards;
- d. failing to comply with the legal obligations necessarily incorporated into the agreements; and
- e. failing to ensure the confidentiality and integrity of the electronic PII that Defendant created, received, maintained, and transmitted.

125. In these and other ways, Defendant violated its duty of good faith and fair dealing.

126. Defendant's material breaches were the direct and proximate cause of Plaintiff's and Class members' injuries (as detailed *supra*).

127. Plaintiff and Class members performed as required under the relevant agreements, or such performance was waived by Defendant's conduct.

FOURTH CAUSE OF ACTION
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

128. Plaintiff incorporates by reference Paragraphs 1 through 82 as if fully set forth herein.

129. Given the relationship between Defendant and Plaintiff and Class members, where Defendant became guardian of Plaintiff's and Class members' PII, Defendant became a fiduciary by its undertaking and guardianship of the PII, to act primarily for Plaintiff and Class members, (1) for the safeguarding of Plaintiff and Class members' PII; (2) to timely notify Plaintiff and Class members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

130. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of Defendant's relationship with them—especially to secure their PII.

131. Because of the highly sensitive nature of the PII, Plaintiff and Class members would not have entrusted Defendant, or anyone in Defendant's position, to retain their PII had they known the reality of Defendant's inadequate data security practices.

132. Defendant breached its fiduciary duties to Plaintiff and Class members by failing to sufficiently encrypt or otherwise protect Plaintiff's and Class members' PII.

133. Defendant also breached its fiduciary duties to Plaintiff and Class members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

134. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and Class members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

FIFTH CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

135. Plaintiff incorporates by reference Paragraphs 1 through 82 as if fully set forth herein.

136. This claim is pleaded in the alternative to the breach of implied contract claim.

137. Plaintiff and Class members conferred a benefit upon Defendant. After all, Defendant benefitted from using their PII to provide medical services.

138. Defendant appreciated or had knowledge of the benefits it received from Plaintiff and Class members. And Defendant benefited from receiving Plaintiff's and Class members' PII, as this was used to provide medical services.

139. Plaintiff and Class members reasonably understood that Defendant would use adequate cybersecurity measures to protect the PII that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

140. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class members' PII.

141. Instead of providing a reasonable level of security, or retention policies, that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiff and Class members by utilizing cheaper, ineffective security measures. Plaintiff and Class members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

142. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff's and Class members' payment because Defendant failed to adequately protect their PII.

143. Plaintiff and Class members have no adequate remedy at law.

144. Defendant should be compelled to disgorge into a common fund—for the benefit of Plaintiff and Class members—all unlawful or inequitable proceeds that it received because of its misconduct.

SIXTH CAUSE OF ACTION
Violation of O.C.G.A. § 13-6-11
(On Behalf of Plaintiff and the Class)

145. Plaintiff incorporates by reference Paragraphs 1 through 82 as if fully set forth herein.

146. Defendant through its actions alleged and described herein acted in bad faith, was stubbornly litigious, or caused Plaintiff and the Class unnecessary trouble and expense with respect to the events underlying this litigation.

147. Section 5 of the FTC Act prohibits “unfair...practices in or affecting commerce” including, as interpreted and enforced by the FTC, the unfair act or practice by companies such as Defendant for failing to implement and use reasonable measures to protect PII.

148. Defendant violated Section 5 of the FTC ACT by failing to use reasonable measures to protect PII and not complying with the industry standards. Defendant’s conduct was particularly unreasonable given the nature and amount of PII that it obtained and stored and the foreseeable consequences of a data breach.

149. Defendant also has a duty under the Georgia Constitution (“the Constitution”) which contains a Right to Privacy Clause, Chapter 1, Article 1, to protect its users’ private information. The Georgia Constitution states, “no person shall be deprived of life, liberty, or property except by due process of law.” Moreover, the Georgia Constitution identifies certain invasions of privacy, including the Public Disclosure of Private Life which prohibits the public disclosure of private facts.

150. This duty has been recognized by the Georgia Supreme Court in the Restatement of the Law of Torts (Second) §652A which specifically recognized four

common law invasion of privacy claims in Georgia, which include 1) appropriation of likeness; 2) intrusion on solitude or seclusion; 3) public disclosure of private facts; and 4) false light.

151. Defendant's implementation of inadequate data security measures, its failure to resolve vulnerabilities and deficiencies, and its abdication of its responsibility to reasonably protect data it required Plaintiff and the Class to provide and store on its own servers constitutes a violation of the Georgia Constitution and the Restatement of the Law of Torts (Second).

152. Defendant knew or should have known that it had a responsibility to protect the PII it required Plaintiff and the Class to provide and stored, that it was entrusted with this PII, and that it was the only entity capable of adequately protecting the PII.

153. Despite that knowledge, Defendant abdicated its duty to protect the PII it required Plaintiff and the Class to provide and that it stored.

154. As a direct and proximate result of Defendant's actions, Plaintiff's and the Class Members' PII was stolen. As further alleged above, the Data Breach was a direct consequence of Defendant's abrogation of data security responsibility and its decision to employ knowingly deficient data security measures that knowingly left the PII unsecured. Had Defendant adopted reasonable data security measures, it could have prevented the Data Breach.

155. As further described above, Plaintiff and the Class have been injured and suffered losses directly attributable to the Data Breach.

156. Plaintiff and the Class therefore request that their claim for recovery of expenses of litigation and attorneys' fees be submitted to the jury, and that the Court enter a judgment awarding their expenses of litigation and attorneys' fees pursuant to O.C.G.A. § 13-6-11.

PRAYER FOR RELIEF

Plaintiff and Class members respectfully request judgment against Defendant and that the Court enter an order:

- A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing his counsel to represent the Class;
- B. Awarding declaratory and other equitable relief as necessary to protect the interests of Plaintiff and the Class;
- C. Awarding injunctive relief as necessary to protect the interests of Plaintiff and the Class;
- D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen PII;

- E. Awarding Plaintiff and the Class damages including applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;
- F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;
- G. Awarding attorneys' fees and costs pursuant to O.C.G.A. § 13-6-11, or as otherwise permitted by law;
- H. Awarding prejudgment and post-judgment interest, as provided by law;
- I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and
- J. Granting other relief that this Court finds appropriate.

DEMAND FOR JURY TRIAL

Plaintiff demands a jury trial for all claims so triable.

Date: June 4, 2024

Respectfully submitted,

/s/ N. Nickolas Jackson

N. Nickolas Jackson

Georgia Bar No. 841433

J. Benjamin Finley

Georgia Bar No. 261504

THE FINLEY FIRM, P.C.

3535 Piedmont Rd.

Building 14, Suite 230

Atlanta, GA 30305

Phone: (404) 978-6971

Fax: (404) 320-9978
njackson@thefinleyfirm.com
bfinley@thefinleyfirm.com

STRAUSS BORRELLI PLLC

Raina Borrelli (*pro hac vice* forthcoming)
980 N. Michigan Ave., Suite 1601
Chicago, IL 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109
raina@straussborrelli.com

Attorneys for Plaintiff and Proposed Class

CERTIFICATE OF COMPLIANCE

I certify that the foregoing pleading has been prepared with Times New Roman, 14-point font, in compliance with L.R.5.1B.

/s/ N. Nickolas Jackson

N. Nickolas Jackson